UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/065,452 | 10/18/2002 | Chung-E Wang | | 1359 |

33275 7590 04/14/2006

CHUNG-E WANG
845 WEST COVE WAY
SACRAMENTO, CA 95831

| EXAMINER | |
|---|---|
| TRAN, ELLEN C | |
| **ART UNIT** | **PAPER NUMBER** |
| 2134 | |

DATE MAILED: 04/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/065,452 | WANG, CHUNG-E | |
| | Examiner | Art Unit | |
| | Ellen C. Tran | 2134 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *19 January 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-6* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

*DETAILED ACTION*

1. This action is responsive to communication: filed on 19 January 2066 with acknowledgement of an original application filed 18 October 2002.

2. Claims 1-6 are currently pending in this application. Claims 1, 2, 4, 5, and 6 are independent claims. Claims 5 and 6 have been amended. Claim 7 has been cancelled.

3. An examination of this application reveals that applicant is unfamiliar with patent prosecution procedure. While an inventor may prosecute the application, lack of skill in this field usually acts as a liability in affording the maximum protection for the invention disclosed. Applicant is advised to secure the services of a registered patent attorney or agent to prosecute the application, since the value of a patent is largely dependent upon skilled preparation and prosecution. The Office cannot aid in selecting an attorney or agent.

A listing of registered patent attorneys and agents is available on the USPTO Internet web site http://www.uspto.gov in the Site Index under "Attorney and Agent Roster." Applicants may also obtain a list of registered patent attorneys and agents located in their area by writing to the Mail Stop OED, Director of the U. S. Patent and Trademark Office, PO Box 1450, Alexandria, VA 22313-1450.

4. The claims submitted 19 January 2006 should have been submitted as a separate paper as required by 37 CFR 1.4(c). The paper has been entered. However, all future correspondence must comply with 37 CFR 1.4. When submitting claims a separate sheet of paper is required in addition before each claim applicant should

indicate the status of the claim, for example, attached is how the claims should have been presented.

***Response to Arguments***

5. Applicant's arguments filed 19 January 2006 have been fully considered but they are not persuasive.

In response to applicant's argument on page 2, "The basic idea of my invention is to use well-known, existing compression algorithms to do encryption. Well-defined steps and instruction for accomplishing simultaneous compression and encryption are given in my specification. They are not just abstract manipulation of data". The Office does not agree the 101 rejection is maintained because the applicant has not provided enough detail in the claims how a person of ordinary skill in the art would use the invention and what steps are needed to perform the invention or improvement expected by using the invention.

In response to applicant's argument on page 3, "As my invention, Barbir's idea is to use known, existing compression algorithms to do the encryption. There are two major processes in every compression algorithm, the modeling process and the encoding process. Barbir's idea is to alter the modeling process of the compression algorithm and my idea is to alter the encoding process instead". The Office does not agree with argument as best understood, the two major processes are not given any weight in relation to the claims as described. The claims do not provide enough detail to overcome the Barbir reference.

In response to applicant's second argument on page 3, "Barbir introduces the randomness by updating a modeler's internal state randomly. (So, the probabilities of characters/symbols would be different.)". As best understood the Office does not agree with argument. Applicant is advised when making arguments they should indicate what the prior art of reference does not teach. Barbir does teach altering the initial values, not the Office interprets internal values have the same meaning as initial values.

In response to applicant's third argument on page 3, "In Claim 1, shuffling the initial values of the dition witht the encryption key doesn't change probbilies of characters/symnol ... Barbir introduces the randomness by changing the modler". As best understood the Office does not agree, the claims are interpreted in light of the specification, however limitation from the specification are not placed into the claims nowhere in the claims are probabilities or symbols mentioned.

In response to applicant's argument on page 4 "In '379 col. 7, lines 62-67 Barbir claims that his idea of altering the modeling process can be used with different encoding processes. In my Claim 2, I don't change the modeling process of Lampel-Ziv compression". As best understood the Office disagrees with argument , the applicant is arguing that Barbir does not combine the random shuffle with a Lampel-Ziv as claimed. The Office disagrees see col. 7 line 61 through 8, line 2, 'compressing data can be used in conjunction with the modeling method of the invention'. "Conjunction" is interpreted to have the same meaning as combined.

In response to applicant's second argument on page 4, "In Claim 2, shuffling the initial values of the dictionary with the encryption key doesn't change probabilities of

character/symbols". The Office disagrees as stated above 'As best understood the Office does not agree, the claims are interpreted in light of the specification, however limitation from the specification are not placed into the claims nowhere in the claims are probabilities or symbols mentioned.'

In response to applicant's third argument on page 4, "In '379 col. 11, lines 54-67, Barbir claims that his idea can be a building block of a multi-step compression and encryption. My Claim 2 doesn't involve multi-step compression and encryption". The Office does not agree with argument, applicant's claim two has three steps a, b, and c.

In response to applicant's fourth argument on page 4, "As sted in '379 col. 2, lines 11-23, XORis a well-known operation. My Claim 2 isn't claiming XOR is a new invention. My claim 2 is claiming that the combination of steps a), b), and c) is a new invention". The Office disagrees with argument, col. 2, lines 11-23 was referenced to explain that the stream cipher, also references in col. 5, lines 26-33, is an XOR.

In response to applicant's argument on page 5, "In '379 col. 7, lines 22-45, Barbir uses a random number generator to determine when to update the modeler's internal state ... I use a random number generator to determine the initial values of the dictionary. As best understood the Office disagrees with argument, Barbir and the invention are using the random number generator the same internal state and initial values are interpreted to have the same meaning.

In response to applicant's second argument on page 5, "In '379 col. 7, line 62 through col. 8, lines 44, Barber is claiming that his idea of altering the modeling process can be used with compression algorithms such as LZ compression, RLE etc. In my

claim 4, I change the encoding process (not the modeling process) by altering the Huffman tree with an encryption key". As best understood the Office disagrees with argument, the applicant is trying to place limitations from the specification into the claims.

In response to applicant's third argument on page 5, "In '379 col. 7, lines 22067, Barbir uses a random number generator to determine when to update the modeler's internal state, ... In my Claim 5, I use an encryption key to alter the Huffman tree and thus alter the encoding process". As best understood the Office does not agree as explained in Barbir the encryption and compression processes can be used in conjunction, in col. 8, lines 36-67 it is explained how an encryption key can be used to alter the values.

In response to applicant's fourth argument on page 5, "I use an encryption key to alter the encoding process". The Office disagrees with argument, there is no difference in the alteration of Barbir with respect to the applicant's invention.

In response to applicant's argument on page 6, "Barbir describes the general idea of the well-known arithmetic coding and his new modeling method. In this claim, swapping left child with the right child of an interior node doesn't change". As best understood the Office does not agree with argument, nowhere in the claims are these limitations implied.

In response to applicant's second argument on page 6, "In '379 col. 6, lines 10 through col. 7, line 21, Barbir describes the general idea of the well-known arithmetic

coding and his new modeling method". As stated above 'As best understood the Office does not agree with the argument nowhere in the claims are theses limitation implied'.

In response to applicant's third argument on page 6, "In '379 col. 6, lines 37-55, Barbir describes the basic idea of his modeling method. In this claim changing the order of diving an interval into smaller intervals with an encryption key doesn't change probabilities of characters/symbols. It only changes the result of the encoding". As best understood, the Office disagrees with argument more detail is needed in the claims to make sense of applicant's arguments to overcome the cited prior art reference of Barbir.

6. This action is a **final rejection** and is intended to close the prosecution of this application. Applicant's reply under 37 CFR 1.113 to this action is limited either to an appeal to the Board of Patent Appeals and Interferences or to an amendment complying with the requirements set forth below.

If applicant should desire to appeal any rejection made by the examiner, a Notice of Appeal must be filed within the period for reply identifying the rejected claim or claims appealed. The Notice of Appeal must be accompanied by the required appeal fee.

If applicant should desire to file an amendment, entry of a proposed amendment after final rejection cannot be made as a matter of right unless it merely cancels claims or complies with a formal requirement made earlier. Amendments touching the merits of the application which otherwise might not be proper may be admitted upon a showing a good and sufficient reasons why they are necessary and why they were not presented earlier.

A reply under 37 CFR 1.113 to a final rejection must include the appeal from, or cancellation of, each rejected claim. The filing of an amendment after final rejection, whether or not it is entered, does not stop the running of the statutory period for reply to the final rejection unless the examiner holds the claims to be in condition for allowance. Accordingly, if a Notice of Appeal has not been filed properly within the period for reply, or any extension of this period obtained under either 37 CFR 1.136(a) or (b), the application will become abandoned.

### *Claim Rejections - 35 USC § 101*

7. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

8. Claims 1-6 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Each claim teaches solely to the abstract manipulation of data.

### *Claim Rejections - 35 USC § 102*

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

10. **Claims 1-6,** are rejected under 35 U.S.C. 102(b) as being anticipated by Barbir U.S. Patent No. 6,122,379 (hereinafter '379).

**As to independent claim 1, "A method of introducing randomness into the process of the dictionary encoding of Lampel-Ziv data compression"** is taught in '379 col. 7, lines 62-67;

**"by shuffling the initial values of the dictionary with the encryption key"** is shown in '379 col. 5, lines 26-33.

**As to independent claim 2, "A method for combining a random shuffle with a Lampel-Ziv data compression to achieve a simultaneous data compression and encryption, comprised of the following steps:"** is disclosed in '379 col. 7, lines 62-67;

**"a) use the encryption key to shuffle the initial values of the dictionary randomly"** is shown in '379 col. 5, lines 26-33;

**"b) compress the input string normally"** is taught in '379 col. 11, lines 54-67;

**"c) perform the bit-wise XOR operation on the compressed result and the encryption key"** is shown in '379 col. 5, lines 26-33 and col. 2, lines 11-23.

**As to dependent claim 3, "where step a) is comprised of the following step: a) If the dictionary doesn't have any initial values, initialize the dictionary with a particular set of values and then use the encryption key to shuffle the dictionary"** is disclosed in '379 col. 7, lines 22-45.

**As to independent claim 4, "A cryptographic method of concealing information in the process of Huffman coding by altering the Huffman tree with an encryption key"** is taught in '379 col. 7, line 62 through col. 8, line 44.

**As to independent claim 5, "A method of shuffling the Huffman tree with an encryption key comprised of the following steps:" "** is taught in '379 col. 7, lines 22-67;

**"a) associate each interior node with a bit of the encryption key"** is shown in '379 col. 8, lines 36-67.

**"b) Swap the left child and the right child of an interior node, if the corresponding encryption bit is 1"** is disclosed in '379 col. 6, lines 10 through
col. 7, line 21.

**As to independent claim 6, "A method of introducing randomness into the process of the arithmetic coding by shuffling the interval table with an encryption key"** is taught in '379 col. 6, lines 10 through col. 7, line 21;

"that is, a method of introducing randomness into the process of the arithmetic coding by changing the order of dividing an interval into smaller intervals with an encryption key" is shown in '379 col. 6, lines 37-55.

*Conclusion*

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed

within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

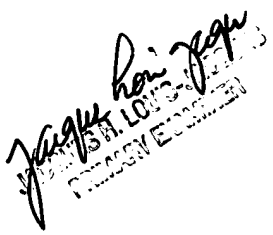
11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:00 am to 2:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques H. Louis-Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ECT

Ellen Tran
Patent Examiner
Technology Center 2134
9 April 2006



This listing of claims will replace all prior versions and listings of claims in this application.

1. (Original) A method of introducing randomness into the process of the dictionary encoding of Lampel-Ziv data compression by shuffling the initial values of the dictionary with the encryption key.

2. (Original) A method for combining a random shuffle with a Lampel-Ziv data compression to achieve a simultaneous data compression and encryption, comprised of the following steps:

a) use the encryption key to shuffle the initial values of the dictionary randomly

b) compress the input string normally

c) perform the bit-wise XOR operation on the compressed result and the encryption key.

3. (Original) A method as defined in claim 2, where step a) is comprised of the following step:

a) If the dictionary doesn't have any initial values, initialize the dictionary with a particular set of values and then use the encryption key to shuffle the dictionary.

4. (Original) A cryptographic method of concealing information in the process of Huffman coding by altering the Huffman tree with an encryption key.

5. (Currently Amended) A method of shuffling the Huffman tree with an encryption key comprised of the following steps:

a) associate each interior node with a bit of the encryption key

b) Swap the left child and the right child of an interior node, if the corresponding encryption bit is 1.

6. (Currently Amended) ~~b) Swap the left child and the right child of an interior node, if the corresponding encryption bit is 1.~~ A method of introducing randomness into the process of the arithmetic coding by shuffling the interval table with an encryption key that is, a method of introducing randomness into the process of the arithmetic coding by changing the order of dividing an interval into smaller intervals with an encryption key.

7. (Cancelled)